

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2003-204338
(P2003-204338A)

(43)公開日 平成15年7月18日 (2003.7.18)

(51)Int.Cl.
H 0 4 L 12/28

識別記号
3 0 0

F I
H 0 4 L 12/28

テマコード(参考)
3 0 0 Z 5 K 0 3 3
3 0 0 A

審査請求 有 請求項の数11 O.L (全 14 頁)

(21)出願番号 特願2002-2419(P2002-2419)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(22)出願日 平成14年1月9日 (2002.1.9)

(72)発明者 可知 靖司

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100088328

弁理士 金田 哲之 (外2名)

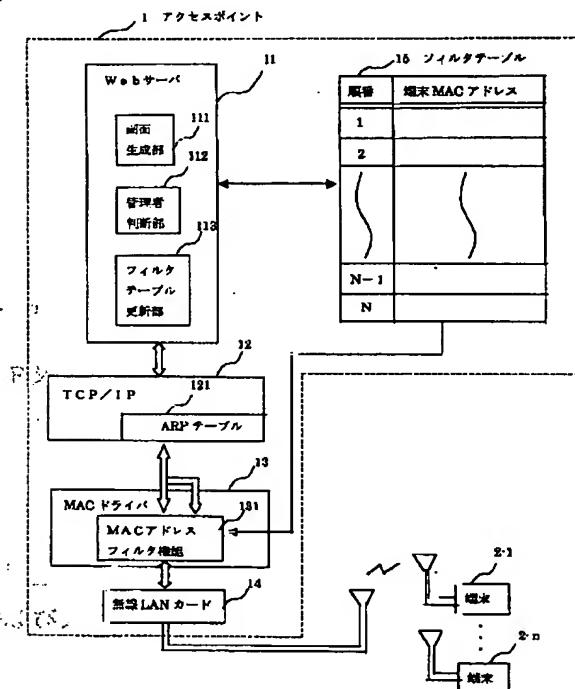
Fターム(参考) 5K033 AA08 DA17 DB16 EC03

(54)【発明の名称】 無線LANシステム、アクセス制御方法およびプログラム

(57)【要約】

【課題】 認証のための処理が煩雑になることがなく、会議の参加者の中からシステム管理者を設定することができる無線LANシステムを提供する。

【解決手段】 任意の場所に設置可能なアクセスポイント1と、アクセスポイント1と無線により相互通信可能に接続される複数の端末2-1～2-nとを有する無線LANシステムであって、アクセスポイント1はサーバ1-1を有し、サーバ1-1は、端末2-1～2-nのうちの当該サーバ1-1に最初にアクセスしてきた端末の利用者をシステム管理者として扱い、それ以外の端末の利用者については、上記システム管理者によって当該サーバ1-1へのアクセスが制限される一般ユーザとして扱うように構成されている。



【特許請求の範囲】

【請求項1】 任意の場所に設置可能なアクセスポイントと、該アクセスポイントと無線により相互通信可能に接続される複数の端末とを有する無線LANシステムであって、

前記アクセスポイントはサーバを有し、
前記サーバは、当該サーバにアクセスしてきた前記複数の端末のうちの所定の端末の利用者をシステム管理者として扱い、それ以外の端末の利用者については、前記システム管理者によって当該サーバへのアクセスが制限される一般ユーザとして扱うように構成されている無線LANシステム。

【請求項2】 所定の端末が、サーバに最初にアクセスしてきた端末であることを特徴とする請求項1に記載の無線LANシステム。

【請求項3】 アクセスポイントはフィルタテーブルをさらに有し、
サーバは、複数の端末のうちの当該サーバにアクセスしてきた端末のMACアドレスをそのアクセスの順番と対応づけて前記フィルタテーブルに登録し、前記フィルタテーブルに最も早い順番でMACアドレスが登録された端末をシステム管理者として扱うことを特徴とする請求項2に記載の無線LANシステム。

【請求項4】 アクセスポイントは、複数の端末のいずれかからパケットが送出されると、該送出されたパケットについて、その送信元の端末のMACアドレスを検査するフィルタ処理手段をさらに有し、

サーバは、当該サーバにアクセスしてきた端末のうち、システム管理者によってアクセス許可の設定がなされた端末のMACアドレスのみを前記フィルタテーブルに登録し、

前記フィルタ処理手段は、前記送出されたパケットの、送信元の端末のMACアドレスが前記フィルタテーブルに登録されている場合、もしくは、前記送出されたパケットが前記サーバへのアクセスである場合にのみ、そのパケットを通すことを特徴とする請求項3に記載の無線LANシステム。

【請求項5】 所定の端末が、サーバにアクセスしてきた端末のうち、自身がシステム管理者となる旨の入力をした端末であることを特徴とする請求項1に記載の無線LANシステム。

【請求項6】 任意の場所に設置可能なアクセスポイントと、該アクセスポイントと無線により相互通信可能に接続される複数の端末とを有する無線LANシステムにおいて行われるアクセストリート方法であって、

前記アクセスポイント内に設置されたサーバにアクセスした前記複数の端末のうちの所定の端末の利用者をシステム管理者として扱い、それ以外の端末の利用者については、前記システム管理者によって前記サーバへのアクセスが制限される一般ユーザとして扱うアクセストリート方

法。

【請求項7】 所定の端末が、サーバに最初にアクセスした端末であることを特徴とする請求項6に記載のアクセストリート方法。

【請求項8】 所定の端末が、サーバにアクセスした端末のうち、自身がシステム管理者となる旨の入力をした端末であることを特徴とする請求項6に記載のアクセストリート方法。

【請求項9】 任意の場所に設置可能なアクセスポイントと、該アクセスポイントと無線により相互通信可能に接続される複数の端末とを有する無線LANシステムにおいて用いられるプログラムであって、

前記アクセスポイント内に設置されたサーバにアクセスした前記複数の端末のうちの所定の端末の利用者をシステム管理者として扱う処理と、

前記所定の端末以外の端末の利用者を、前記システム管理者によって前記サーバへのアクセスが制限される一般ユーザとして扱う処理とを、前記サーバのコンピュータに実行させるプログラム。

【請求項10】 所定の端末が、サーバに最初にアクセスした端末であることを特徴とする請求項9に記載のプログラム。

【請求項11】 所定の端末が、サーバにアクセスした端末のうち、自身がシステム管理者となる旨の入力をした端末であることを特徴とする請求項9に記載のプログラム。

【発明の詳細な説明】

【0.001】

【発明の属する技術分野】本発明は、データ通信システムに関し、特に無線LAN (Local Area Network) システムに関する。さらに、本発明は、そのようなシステムにおいて用いられる、アクセストリート方法およびプログラムに関する。

【0.002】

【従来の技術】最近では、社内のちょっとした会議でも、各参加者が携帯情報端末、例えばノート型PC (パソコン用コンピュータ) 端末を持ち寄って、必要な情報をやり取りするケースが多くなってきた。こういった場合、参加者の間で共有する情報 (例えば、参加者に配布される、会議に必要な情報で、ファイル形式でデータ保存される。) は、例えばコンパクトフラッシュ (登録商標) (カードメモリ) などのメディアを用いて各参加者に渡されるが、参加者の人数が多くなると、そういったメディアを用いたファイルの共有は非常に面倒である。そこで、上記のような会議において、参加者の各PC端末をネットワークを介して相互に通信可能に接続することができるLANが導入されるようになってきた。

【0.003】LANは、基本的に、1つのサーバと、これに相互通信可能に接続される複数の端末 (クライアント) とから構成されており、伝送媒体の違いから、有線

LANと無線LANに分類される。有線LANは、通信ケーブルなどを予め敷設しておく必要があり、会議に使用される社内のすべての部屋にそのような敷設を行うことはコストなどの面から難しいことから、上記のような会議への適用は困難である。これに対して、無線LANは、通信ケーブルなどの敷設は必要なく、持ち運び可能な一時設置アクセスポイント (Access Point : AP) を使用することで、必要なネットワークを任意の場所で構築することができるので、上記のような会議への適用は容易である。

【0004】無線LANの導入に際して問題となるのが、セキュリティである。会議で扱われるデータは、秘匿性の高いものであり、外部に漏れることを避けるためには、無線LANに対する第三者からのアクセスを何らかの形で制限する必要がある。このような制限を行うために、通常は、無線LANのネットワークOS (オペレーティングシステム) がセキュリティ機能を備えている。

【0005】セキュリティ機能には、例えば、登録されたユーザが正しいパスワードを提示した場合にのみサーバへのログインを認めるネットワークアクセスの制御や、ファイルへのアクセス権を特定のユーザに限定するファイルへのアクセス制御などの他、ユーザの登録などを管理するユーザ管理やシステム管理などを特別な権限を持つシステム管理者に限定する制御がある。システム管理者は、このセキュリティ機能を用いて、決められたクライアントに対してのみサーバへのアクセスを許可することができ、これにより、第三者による不正なアクセスを制限することができる。

【0006】また、よりセキュリティを高めるために、MAC (Medium Access Control : 媒体アクセス制御) アドレスを検査するパケットフィルタ機能により、第三者による不正なアクセスを制限するものがある。ここで、MACアドレスは、物理アドレスであって、送信先アドレスおよび送信元アドレスである。図8は、そのようなMACアドレスを利用したアクセス制限を行う無線LANシステムの概略構成図である。

【0007】図8において、無線LANの基地局としてのアクセスポイント (AP) 101と、AP 101に帰属する移動端末局としての複数のステーション (Station : STA) 102-1～102-kとから構成されている。ここに示す無線LANシステムは、IEEE802.11で定義するところのインフラストラクチャ方式を採用するものであって、無線LANネットワークの最小単位 (BBS (Basic ServiceSet) 4) を構成する。

【0008】BBS 4内におけるAP 101は、各STA 102-1～102-kがAP 101に同期するための情報を含むビーコンフレームを周期的にBBS 4内にブロードキャスト送信する。このビーコンフレームを受信したBBS 4内の各STA 102-1～102-k

は、通信開始時にAP 101に対して認証要求を行い、AP 101により認証許可を受けた後、AP 101との間で通信を行うことが可能となる。なお、図8に示したシステムにおいて、AP 101は、「portal」となっているが、この「portal」は、IEEE802.11以外のLANプロトコルとのプロトコル変換機能をAP 101に付加していることを意味する。このプロトコル変換機能によりAP 101と有線LANであるイーサネット (登録商標) 105との接続が可能になっている。

【0009】上記AP 101による認証は、MACアドレスによるパケットフィルタ機能を利用した公開鍵認証である。AP 101は、認証をしたSTAのMACアドレスが登録される公開鍵管理テーブルと、自らの秘密鍵であるAP秘密鍵と、これに対応する公開鍵であるAP公開鍵と、これを付したAPユーザ証明書とを有する。各STA 102-1～102-kは、公開鍵認証を受けたAP 101のMACアドレスが登録されるAP情報管理テーブルと、自らの秘密鍵であるSTA秘密鍵と、これに対応する公開鍵であるSTA公開鍵と、これを付したSTAユーザ証明書とを有する。

【0010】各STA 102-1～102-kは、以下のような手順でAP 101による公開鍵認証を受ける。各STA 102-1～102-kの公開鍵認証は同じ手順で行われることから、以下の説明では、STA 102-1を例に挙げて手順を説明する。

【0011】STA 102-1は、無線通信を行おうとするAP 101のMACアドレスが自身の保持するAP情報管理テーブル内にあるかどうかを確認する。AP 101のMACアドレスがない場合は、STA 102-1は、AP 101に対して公開鍵認証要求を行い、AP 101のMACアドレスがある場合には、STA 102-1は、AP 101に対して公開鍵再認証要求を行う。

【0012】公開鍵認証要求がなされた場合は、まず、その要求を受信したAP 101がSTA 102-1に対してAPユーザ証明書を送信する。次いで、STA 102-1が、受信したAPユーザ証明書を検証した後、そのAPユーザ証明書に添付されたAP公開鍵を用いてSTAユーザ証明書を暗号化した暗号化STAユーザ証明書をAP 101へ送信する。次いで、AP 101が、受信した暗号化STAユーザ証明書をAP秘密鍵で復号化して元のSTAユーザ証明書を再生し、この再生したSTAユーザ証明書を検証した後に、そのSTAユーザ証明書に添付されたSTA公開鍵を用いて、前回の処理でSTA 102-1に対して作成してあった共通鍵を暗号化し、この暗号化共通鍵をSTA 102-1へ送信する。最後に、STA 102-1が、受信した暗号化共通鍵をSTA公開鍵で復号化して元の共通鍵を再生する。これにより、STA 102-1は、再生した公開鍵を用いてAP 101とのフレーム暗号化通信を行うことが可能となる。

【0013】一方、公開鍵再認証要求がなされた場合は、まず、その要求を受信したAP101が、STA102-1のMACアドレスおよびSTA公開鍵の両方が自身の保持する公開鍵管理テーブル内に存在するかどうかを確認し、両方が存在した場合には、STA102-1に対して指定する新たな共通鍵を生成し、この生成した新共通鍵をSTA公開鍵で暗号して暗号化新共通鍵を生成し、この生成した暗号化新共通鍵をSTA102-1に送信して認証許可を通知する。次いで、STA102-1が、受信した暗号化新共通鍵をSTA秘密鍵で復号化して元の新共通鍵を再生する。これにより、STA102-1は、再生した新共通鍵を用いてAP101とのフレーム暗号化通信を行うことが可能となる。

【0014】

【発明が解決しようとする課題】上述したように、従来の無線LANでは、予め定めたシステム管理者が、利用者に対してのみアクセスを許可し、第三者による不正なアクセスを制限するようになっている。しかし、この場合は、システム管理者が固定であるため、システム管理者が会議に参加しない場合は、会議の参加者が、いちいちシステム管理者に対してアクセス許可を得る必要がある、という問題がある。加えて、システム管理者によるアクセス制限は、通常、IDとパスワードにより行われるため、会議の度に、参加者は、システム管理者からIDとパスワードを取得する必要があり、アクセスに必要な手続きが煩雑になる、という問題もある。

【0015】図8に示したシステムのように、MACアドレスを検査するパケットフィルタ機能を用いることで、よりセキュリティを高めることができる。しかし、このシステムの場合は、各端末(クライアント)に対して公開鍵と秘密鍵とを用いた認証を行う必要があり、やはり処理が煩雑になるという問題がある。

【0016】本発明の目的は、上記各問題を解決し、認証のための処理が煩雑になることがなく、会議の参加者の中からシステム管理者を設定することのできる、無線LANシステム、アクセス制御方法およびプログラムを提供することにある。

【0017】

【課題を解決するための手段】上記目的を達成するため、本発明の無線LANシステムは、任意の場所に設置可能なアクセスポイントと、該アクセスポイントと無線により相互通信可能に接続される複数の端末とを有する無線LANシステムであって、前記アクセスポイントはサーバを有し、前記サーバは、当該サーバにアクセスしてきた前記複数の端末のうちの所定の端末の利用者をシステム管理者として扱い、それ以外の端末の利用者については、前記システム管理者によって当該サーバへのアクセスが制限される一般ユーザとして扱うように構成されていることを特徴とする。

【0018】本発明のアクセス制御方法は、任意の場所

に設置可能なアクセスポイントと、該アクセスポイントと無線により相互通信可能に接続される複数の端末とを有する無線LANシステムにおいて行われるアクセストリ方法であって、前記アクセスポイント内に設置されたサーバにアクセスした前記複数の端末のうちの所定の端末の利用者をシステム管理者として扱い、それ以外の端末の利用者については、前記システム管理者によって前記サーバへのアクセスが制限される一般ユーザとして扱うことを特徴とする。

【0019】本発明のプログラムは、任意の場所に設置可能なアクセスポイントと、該アクセスポイントと無線により相互通信可能に接続される複数の端末とを有する無線LANシステムにおいて用いられるプログラムであって、前記アクセスポイント内に設置されたサーバにアクセスした前記複数の端末のうちの所定の端末の利用者をシステム管理者として扱う処理と、前記所定の端末以外の端末の利用者を、前記システム管理者によって前記サーバへのアクセスが制限される一般ユーザとして扱う処理とを、前記サーバのコンピュータに実行させることを特徴とする。

【0020】上記のとおりの本発明においては、例えば、サーバに最初にアクセスしてきた端末の利用者がシステム管理者とされるので、会議の参加者のだれかがシステム管理者になる。したがって、システム管理者が予め固定された従来のシステムのように、会議の参加者が、いちいちシステム管理者に対してアクセス許可を得る必要はない。

【0021】また、本発明によれば、システム管理者は会議の参加者のうちの一人であり、このシステム管理者により他の端末からのアクセスを制限するようになっている。システム管理者は、通常、会議の参加者に対してのみアクセスが許可することから、第3者による不正なアクセスは拒否されることになる。また、システム管理者による他の端末からのアクセスの制限にIDとパスワードによる認証は必要としないので、従来のようにアクセスに必要な手続きが煩雑になることはない。

【0022】

【発明の実施の形態】次に、本発明の実施形態について図面を参照して説明する。

【0023】図1は、本発明の一実施形態の無線LANシステムの概略構成を示すブロック図である。このシステムは、任意の場所に一時的に設置されるアクセスポイント(AP)1と、このAP1と相互に無線通信可能な複数の端末(クライアント)2-1～2-nとを有する。各端末2-1～2-nは、所定の無線通信機能(例えば無線LANカード)を備える、ノート型PC端末である。

【0024】AP1は、Webサーバ11、TCP/IP(Transmission Control Protocol / Internet Protocol)12、MACドライバ13、無線LANカード1

4およびフィルターテーブル15を有する。フィルターテーブル15には、Webサーバ11への接続要求のあった端末のMACアドレスが、接続要求を受けた順に登録される。このフィルターテーブル15へのMACアドレスの登録はWebサーバ11により行われる。ただし、AP1起動時には、フィルターテーブル15には何もMACアドレスは登録されていないものとする。

【0025】TCP/IP12、MACドライバ13および無線LANカード14は、プロトコルスタックである。TCP/IP12は、インターネットワーキングでよく知られた通信プロトコルであって、AP1と各端末2-1～2-nとの間の相互接続を可能とする。このTCP/IP12内部には、IPアドレスとMACアドレスとの対応をとるためのARP(Address Resolution Protocol)テーブル121が備えられている。Webサーバ11は、このARPテーブル121を用いて、各端末2-1～2-nから送出されたパケットに含まれる環境変数のIPアドレスから接続要求をした端末のMACアドレスを取得することが可能である。

【0026】無線LANカード14は、各端末2-1～2-nとの無線通信を可能にするためのものである。MACドライバ13は、この無線LANカード14による無線通信を制御するためのデバイスドライバであって、内部にMACアドレスフィルタ機能131を有する。MACアドレスフィルタ機能131は、上記Webサーバ11と同様、ARPテーブル121を用いて、各端末2-1～2-nから送出されたパケットに含まれる環境変数のIPアドレスから接続要求をした端末のMACアドレスを取得することが可能であり、取得したMACアドレスと現在のフィルターテーブル15の内容を参照してパケットの通過許可/禁止を行う。ただし、MACアドレスフィルタ機能131は、フィルターテーブル15にMACアドレスが登録されていない端末からのパケットで、Webサーバ11宛てのパケットについては無条件に通過させる。

【0027】Webサーバ11は、画面生成部11、管理者判断部112およびフィルターテーブル更新部113を有する。フィルターテーブル更新部113は、Webサーバ11へアクセス要求した端末のMACアドレスを、受付順にフィルターテーブル15に登録する。例えば、最初に受け付けた端末のMACアドレスは、フィルターテーブル更新部113によって順番1の欄に登録される。管理者判断部112は、フィルターテーブル15に最初に登録されたMACアドレス、すなわち順番1の欄に登録されたMACアドレスをシステム管理者の端末、それ以外の順番2～Nに登録されたMACアドレスを一般ユーザの端末と判断する。画面生成部11は、管理者判断部112によってシステム管理者と判断された端末に対して、システム管理者である旨の通知を行う。また、画面生成部11は、システム管理者以外の端末からWebサ

ーバ11へ初めてのアクセス要求があった際には、システム管理者の端末に、そのアクセス要求した端末に対するアクセス許可/禁止設定画面を表示して設定作業を促すとともに、その設定結果をフィルターテーブル15に書き込む。さらに、画面生成部11は、アクセス要求した端末に対して、システム管理者に対してアクセス許可を要求中である旨の表示、その結果(許可/禁止)の表示などを行う。

【0028】次に、この無線LANシステムの動作について説明する。以下、端末2-1がシステム管理者の端末、それ以外の端末が一般ユーザの端末となるように設定する場合の動作を例にあげて具体的に説明する。

【0029】AP1起動直後、まだ、どの端末からもWebサーバ11へのアクセス要求が出されていない状態で、端末2-1からWebサーバ11に対してアクセス要求を行うと、端末2-1からのパケットは無線LANカード14を通じてMACドライバ13に届く。この時点では、フィルターテーブル15には何も登録されておらず、また、端末2-1から送信されたパケットはWebサーバ11宛てのものであるため、その送信パケットはMACアドレスフィルタ機能131による制限を受けることなく、そのままTCP/IP12を通じてWebサーバ11に届く。

【0030】Webサーバ11では、端末2-1からのパケットを受信すると、まず、受信したパケットの環境変数から取得したIPアドレスからARPテーブル121を用いてMACアドレスを取得する。次いで、フィルターテーブル更新部113がフィルターテーブル15の登録内容を調べる。この時点では、フィルターテーブル15には何も登録されていないため、フィルターテーブル更新部113は、MACアドレスをフィルターテーブル15の順番1の欄に登録する。そして、画面生成部111が、端末2-1に対して、システム管理者に設定された旨の通知を行う。このシステム管理者設定通知により、端末2-1の所有者は自分がシステム管理者になってことを確認することができる。

【0031】上記のシステム管理者設定の後、端末2-1以外の端末、例えば端末2-nからWebサーバ11に対してアクセス要求を行うと、端末2-nからのパケットは無線LANカード14を通じてMACドライバ13に届く。この時点では、フィルターテーブル15の順番1の欄に端末2-1のMACアドレスが登録されているだけで、端末2-nに関するMACアドレスは登録されておらず、また、端末2-nから送信されたパケットはWebサーバ11宛てのものであるため、その送信パケットはMACアドレスフィルタ機能131による制限を受けることなく、そのままTCP/IP12を通じてWebサーバ11に届く。

【0032】Webサーバ11では、端末2-nからのパケットを受信すると、まず、受信したパケットの環境

変数から取得したIPアドレスからARPテーブル121を用いてMACアドレスを取得する。次いで、フィルターテーブル更新部113が、フィルターテーブル15の登録内容を調べ、管理者判断部112が、その登録内容に基づいて、パケットを送信した端末2-nがシステム管理者のものであるかどうかを判断する。具体的には、管理者判断部112は、取得した端末2-nのMACアドレスと、フィルターテーブル15の順番1の欄に登録されたMACアドレスとが一致するかどうかで、システム管理者の端末かどうかの判断を行う。この時点では、フィルターテーブル15の順番1の欄には端末2-1のMACアドレスが登録されているので、管理者判断部112は、端末2-nからのアクセス要求をシステム管理者以外の端末からのアクセス要求であると判断する。そして、画面生成部111が、システム管理者の端末2-1に対して、端末2-nからのアクセス許可/禁止設定画面を表示させるとともに、端末2-nに対して「管理者に対して許可要求中」の情報表示を行う。

【0033】端末2-1に表示されたアクセス許可/禁止設定画面上で、システム管理者が、アクセスを許可する、あるいは、アクセスを禁止する旨の設定入力を行うと、画面生成部111が、その設定入力結果の情報表示を端末2-nに対して行うとともに、フィルターテーブル更新部113が、フィルターテーブル15の次に空いている順番2の欄に端末2-nのMACアドレスおよび設定入力結果を登録する。例えば、システム管理者が、アクセスを許可する旨の設定入力を行った場合は、端末2-nに「アクセス許可」が表示され、フィルターテーブル15の順番2の欄には、端末2-nのMACアドレスとともに「アクセス許可」が登録される。反対に、システム管理者が、アクセスを禁止する旨の設定入力を行った場合は、端末2-nに「アクセス禁止」が表示され、フィルターテーブル15の順番2の欄には、端末2-nのMACアドレスとともに「アクセス禁止」が登録される。ここでは、フィルターテーブル15の順番2の欄に端末2-nのMACアドレスおよび「アクセス許可」の設定入力結果が登録されたものと仮定する。

【0034】他の端末2-2~2-(n-1)の端末についても、システム管理者設定の後、Webサーバ11へ初めてアクセス要求を行った場合には、上記の端末2-nと同様の手順で、それぞれのMACアドレスおよびシステム管理者によるアクセス許可/禁止の設定結果がフィルターテーブル15に登録される。

【0035】次に、各端末2-1~2-nからのWebサーバ11への2回目以降のアクセスの際の動作について説明する。

【0036】端末2-1からWebサーバ11へ2回目のアクセス要求を行うと、端末2-1からのパケットは無線LANカード14を通じてMACドライバ13に届く。この時点では、フィルターテーブル15の順番1の欄

に端末2-1のMACアドレスが登録されており、しかも、この順番1はシステム管理者であることを示すものであるため、MACアドレスフィルタ機能131は、その送信パケットをそのままTCP/IP12を介してWebサーバ11に送出する。

【0037】Webサーバ11では、パケットを受信すると、まず、受信したパケットの環境変数から取得したIPアドレスからARPテーブル121を用いてMACアドレスを取得する。次いで、フィルターテーブル更新部113が、フィルターテーブル15の登録内容を調べ、管理者判断部112が、その登録内容に基づいて、パケットを送信した端末2-1がシステム管理者のものであるかどうかを判断する。この時点では、フィルターテーブル15の順番1の欄には、端末2-1のMACアドレスが登録されているので、管理者判断部112は、パケットを送信した端末2-1をシステム管理者の端末として取り扱う。これにより、Webサーバ11と端末2-1との間で必要なデータの授受が可能になる。

【0038】一方、端末2-1以外の端末、例えば端末2-nからWebサーバ11へ2回目のアクセス要求を行うと、端末2-nからのパケットは無線LANカード14を通じてMACドライバ13に届く。この時点では、フィルターテーブル15の順番2の欄に端末2-nのMACアドレスが登録されており、しかも、この順番2の欄には「アクセス許可」の設定入力結果が登録されているので、MACアドレスフィルタ機能131は、その送信パケットをそのままTCP/IP12を介してWebサーバ11へ送出する。なお、順番2の欄に登録されている設定入力結果が「アクセス禁止」である場合は、MACアドレスフィルタ機能131は、端末2-nからのパケットを廃棄する。

【0039】Webサーバ11では、パケットを受信すると、まず、受信したパケットの環境変数から取得したIPアドレスからARPテーブル121を用いてMACアドレスを取得する。次いで、フィルターテーブル更新部113が、フィルターテーブル15の登録内容を調べ、管理者判断部112が、その登録内容に基づいて、パケットを送信した端末2-1がシステム管理者のものであるかどうかを判断する。端末2-nのMACアドレスは、フィルターテーブル15の順番2の欄に登録されているため、管理者判断部112は、パケットを送信した端末2-nを、システム管理者によってアクセス許可が許された一般ユーザの端末として取り扱う。これにより、Webサーバ11と端末2-nとの間で必要なデータの授受が可能になる。

【0040】以上のように、本実施形態の無線LANシステムによれば、Webサーバ11は、最初にアクセスしてきた端末をシステム管理者の端末とするようになっているので、会議の参加者のだれかがシステム管理者になることになる。

【0041】また、フィルタテーブル25に登録されていない端末は、Webサーバ21へアクセスを要求する際には、必ず、設定されたシステム管理者によってアクセスの許可/禁止の設定がなされるため、システム管理者が会議の参加者に対してのみアクセスを許可するようすれば、第3者による不正なアクセスを防止することができる。

【0042】

【実施例】図2は、本発明の無線LANシステムの一実施例を示すブロック図である。本実施例のシステムは、図1に示したシステムを、「Windows」（マイクロソフト社製）を搭載したPC上で作成した。「Windows」共有ファイルに対するアクセス制限を行うシステムに適用したもので、その構成は「Windows」共有ファイル20、Webサーバ21、TCP/IP22、MACドライバ23、無線LANカード24およびフィルタテーブル25からなるアクセスポイントと、これに無線により相互通信可能に接続される2台の端末2a、2bとから構成されている。Webサーバ21、TCP/IP22、MACドライバ23、無線LANカード24およびフィルタテーブル25は、図1に示したシステムのものと基本的に同じものである。

【0043】「Windows」共有ファイル20は、例えばUNIX（登録商標）では、SAMBAと呼ばれるアプリケーションで実現することができる。また、Webサーバ21は、UNIXでは、「Apache」というアプリケーションで実現することができる。Webサーバ21は、アクセスを要求した端末に対してWeb画面の表示を行うとともに、前述の実施形態で説明したようにフィルタテーブル25へ必要なデータの登録および参照を行う。

【0044】2台の端末2a、2bは無線LAN端末で、それぞれIPアドレスおよびMACアドレスを以下のように設定している。

【0045】

端末2a: IP=192.168.1.1 MAC=000042-8A9C01
端末2b: IP=192.168.1.2 MAC=000042-8A9C02
ここで、MACアドレス中の「-」は、アドレス表記を見易いものにするために挿入したものである。

【0046】次に、本実施例のシステムの動作を具体的に説明する。図3は、図2のシステムにおけるMACドライバ23のMACアドレスフィルタ機能におけるフィルタ処理手順を示すフローチャートである。図4は、図2のシステムにおけるWebサーバ21の動作を示すフローチャートである。

【0047】まず、端末2aがWebサーバ21にアクセスしたときの動作について説明する。

【0048】端末2aがWebサーバ21にパケットを送信すると、この送信パケットは、無線LANカード24を経由してMACドライバ23に届く。このMACド

ライバ23では、MACアドレスフィルタ機能により、図3に示す以下のような手順でフィルタ処理が行われる。

【0049】ステップS10で、端末2aのMACアドレスがフィルタテーブル25に登録されているかどうかが判断される。この端末2aからWebサーバ21へのアクセスは初めてのアクセスであるため、この時点では、端末2aのMACアドレスはフィルタテーブル25に登録されていない。したがって、このステップS10での判断における分岐は「N」となり、続くステップS12に移行する。なお、端末2aのMACアドレスがフィルタテーブル25に登録されている場合は、分岐は「Y」となり、ステップS11でパケットを通すことになる。

【0050】ステップS12では、端末2aのアクセスがWebサーバへのアクセスかどうかの判断が行われる。この端末2aからのアクセスはWebサーバへのアクセスであるので、このステップS11での判断における分岐は「Y」となり、続くステップS13でパケットを通することになる。なお、Webサーバへのアクセスでない場合は、分岐は「N」となり、続くステップS14でパケットは破棄される。

【0051】上記のようにして、端末2aからのパケットはMACアドレスフィルタ機能によるフィルタ処理を受けた後、TCP/IP22を通ってWebサーバ21に届く。

【0052】次に、端末2aからのパケットを受信したWebサーバ21の動作を、図4を参照して説明する。

【0053】ステップS20で、端末2aからのパケットの環境変数から端末2aのIPアドレス「192.168.1.1」を取得する。続くステップS21で、TCP/IP22内部のARPテーブルを用いてその取得したIPアドレスから端末2aのMACアドレス「000042-8A9C01」を取得する。次いで、ステップS22で、その取得したMACアドレスがフィルタテーブル25に登録されているかどうかを調べる。この時点では、端末2aからのアクセスは初めてのアクセスであるので、フィルタテーブル25には端末2aのMACアドレスは登録されていない。したがって、ステップS22における分岐は「N」となり、続くステップS26でフィルタテーブル25への登録を行う。ここでは、端末2aを当該Webサーバへ最初にアクセスした端末と仮定し、端末2aのMACアドレスをフィルタテーブル25の1番の欄に登録する。

【0054】ステップS26にて端末2aのMACアドレスのフィルタテーブル25への登録がなされると、続いて、ステップS27で、フィルタテーブル25への登録が1番の欄への登録であったかどうかが判断される。ステップS26で、端末2aのMACアドレスをフィルタテーブル25の1番の欄に登録したので、ステップS2

7における分岐は「Y」となり、続くステップS28で端末2aに対して管理者用画面表示を行う。これにより、端末2aの利用者は、システム管理者として他の端末のアクセスの許可/禁止を制限することが可能となる。

【0055】次に、端末2bがWebサーバ21へアクセスした場合の動作について説明する。

【0056】端末2bがWebサーバ21にパケットを送信すると、この送信パケットも、上述の端末2aの場合と同様に、無線LANカード24を経由してMACドライバ23に届く。MACドライバ23では、MACアドレスフィルタ機能により以下のような手順でフィルタ処理が行われる(図3参照)。

【0057】ステップS10で、端末2bのMACアドレスがフィルタテーブル25に登録されているかどうかが判断される。この端末2bからWebサーバ21へのアクセスは初めてのアクセスであるため、この時点では、端末2bのMACアドレスはフィルタテーブル25に登録されていない。したがって、このステップS10での判断における分岐は「N」となり、続くステップS12に移行する。

【0058】ステップS12では、端末2aのアクセスがWebサーバ21へのアクセスかどうかの判断が行われる。この端末2aからのアクセスはWebサーバ21へのアクセスであるので、このステップS11での判断における分岐は「Y」となり、続くステップS13でパケットを通すことになる。

【0059】上記のようにして、端末2bからのパケットはMACアドレスフィルタ機能によるフィルタ処理を受けた後、TCP/IP22を通ってWebサーバ21に届く。

【0060】次に、端末2bからのパケットを受信したWebサーバ21の動作を説明する(図4参照)。

【0061】ステップS20で、端末2bからのパケットの環境変数から端末2bのIPアドレス「192.168.1.2」を取得する。続くステップS21で、TCP/IP22内部のARPテーブルを用いてその取得したIPアドレスから端末2bのMACアドレス「000042-8A9C012」を取得する。次いで、ステップS22で、その取得したMACアドレスがフィルタテーブル25に登録されているかどうかを調べる。この時点では、端末2bからのアクセスは初めてのアクセスであるので、フィルタテーブル25には端末2bのMACアドレスは登録されていない。したがって、ステップS22における分岐は「N」となり、続くステップS26でフィルタテーブル25への登録を行う。フィルタテーブル25の1番の欄には端末2aのMACアドレスがすでに登録されているので、端末2bのMACアドレスは2番の欄に登録される。

【0062】ステップS26にて端末2bのMACアド

レスのフィルタテーブル25への登録がなされると、続いて、ステップS27で、フィルタテーブル25への登録が1番の欄への登録であったかどうかが判断される。ステップS26で、端末2bのMACアドレスをフィルタテーブル25の2番の欄に登録したので、ステップS27における分岐は「N」となり、続くステップS29で端末2aに対して端末2bに関するアクセス要求画面表示を行う。これにより、端末2aの利用者であるシステム管理者は、表示されたアクセス要求画面上で端末2bに対してアクセスの許可/禁止を制限することができる。

【0063】上記ステップS29で、システム管理者が端末2bに対してアクセスの禁止を設定した場合は、Webサーバ21は、上記ステップS26で順番2の欄に登録した端末2bのMACアドレスを削除する。システム管理者が端末2bに対してアクセスの許可を設定した場合は、上記ステップS26で順番2の欄に登録した端末2bのMACアドレスはそのまま保持される。上記ステップS29で、システム管理者が端末2bに対してアクセスの許可を設定した場合の、フィルタテーブル25の登録内容の一例を図5に示す。図5の例では、順番「1」の欄に端末2aのMACアドレス「000042-8A9C01」が登録され、さらに順番「2」の欄に端末2bのMACアドレス「000042-8A9C02」が登録されている。このフィルタテーブル25は、MACアドレスフィルタ機能におけるフィルタ処理の際に用いられ、以降端末2bからのすべてのパケットがこのMACアドレスフィルタ機能を通過することとなる。

【0064】次に、端末2a、2bからの2回目以降のアクセスについて簡単に説明する。

【0065】端末2aからの2回目以降のアクセスの場合は、図3のステップS10の分岐で「Y」となり、端末2aからのパケットがWebサーバ21に届く。Webサーバ21では、図4のステップS22の分岐で「Y」となり、続くステップS23で1番の欄に登録されているか否かの判断がなされる。端末2aのMACアドレスはフィルタテーブル25の1番の欄に登録されているので、この判断における分岐は「Y」となり、続くステップS24で、端末2aに対して再び管理者用画面表示が行われる。

【0066】端末2bからの2回目以降のアクセスの場合は、図3のステップS10の分岐で「Y」となり、端末2bからのパケットがWebサーバ21に届く。Webサーバ21では、図4のステップS22の分岐で「Y」となり、続くステップS23で1番の欄に登録されているか否かの判断がなされる。端末2bのMACアドレスはフィルタテーブル25の2番の欄に登録されているので、この判断における分岐は「Y」となり、続くステップS24で、端末2bに対して一般者用画面表示が行われる。ここで、一般者用画面表示は、例えば、会

議に関する情報一覧である。端末2bの利用者は、その情報一覧から所望の項目、例えばWindows共有ファイル20を選択することで必要な情報を入手することができる。

【0067】なお、システム管理者からアクセス許可を得る前に端末2bからWindows共有ファイル20へ直接アクセスが行われた場合は、図3のステップS10の分岐が「N」となり、続くステップS12の分岐が「N」となって、ステップS14で端末2bからのパケットが廃棄される。

【0068】上述した本実施例の無線LANシステムの構成および動作は一例であり、種々変更が可能である。例えば、図4のステップS29で、端末2aの利用者であるシステム管理者が、表示されたアクセス要求画面上で端末2bに対してアクセスの許可／禁止を制限する設定入力を行った場合に、その設定入力結果をフィルタテーブル25に登録するようにしてもよい。その場合のフィルターテーブル25の一例を図6に示す。図6の例では、順番「1」の欄に端末2aのMACアドレス「000042-8A9C01」が登録され、さらに順番「2」の欄に端末2bのMACアドレス「000042-8A9C02」および設定入力結果「アクセス許可」が登録されている。この場合は、MACアドレスフィルタ機能は、フィルターテーブル25に登録された設定入力結果を参照してフィルタ処理を行うことになる。

【0069】以上説明した実施形態および実施例では、AP起動後、Webサーバに対して最初にアクセスした端末をシステム管理者として設定するようになっているが、本発明はこれに限定されるものではなく、会議の参加者のだれかにシステム管理者を設定することができる。であれば、どのような構成としてもよい。例えば、Webサーバへのアクセス時に、「自分をシステム管理者として登録する」というチェックボックスを設けたアクセス画面が端末に表示されるようにし、このチェックボックスをチェックした形でアクセス要求を行った端末に対してシステム管理者の設定を行うようにしてもよい。

【0070】また、APは、他の有線LANと接続されていてもよい。APが他の有線LANと接続されたシステムとしては、例えば図8に示した従来のシステムに本発明の無線LANシステムの構成を適用したものが考えられる。

【0071】また、アクセスポイント内に設けられるサーバやMACアドレスフィルタ機能、および端末などは、周知のコンピュータシステムによって実現することができる。図7は、そのようなコンピュータシステムの一形態を示すブロック図である。このコンピュータシステムは、プログラムなどを蓄積する記憶装置31、キーボードやマウスなどの入力装置32、CRTやLCDなどの表示装置33、外部との通信を行うモ뎀などの通信装置34、プリンタなどの出力装置35および入力装

置からの入力を受け付けて通信装置、出力装置、表示装置の動作を制御する制御装置(CPU)30から構成されている。例えば、図2のシステムのサーバをこのコンピュータシステムを用いて構成する場合は、記憶装置31に図4に示した処理手順を実行するためのプログラムが予め記憶され、制御装置30がそのプログラムを読み出して実行することになる。なお、プログラムは、不図示の記録媒体(CD-ROM)などで提供されてもよい。

【0072】

【発明の効果】以上説明したように、本発明によれば、システム管理者は会議の参加者の中から設定される。したがって、従来のように会議に参加しないシステム管理者に対していちいちアクセス許可を得る必要がなく、より利用し易いシステムを提供することができる。

【0073】また、本発明によれば、システム管理者は、会議の参加者が利用者となっている端末に対してのみアクセスを許可するので、第3者による不正なアクセスを確実に防止することができる。

【0074】さらに、本発明によれば、システム管理者によるアクセス制限に、IDとパスワードによる認証を必要としないので、処理手順の簡単化、処理時間の短縮を図ることができる。

【図面の簡単な説明】

【図1】本発明の一実施形態の無線LANシステムの概略構成を示すブロック図である。

【図2】本発明の無線LANシステムの一実施例を示すブロック図である。

【図3】図2に示すシステムにおけるMACアドレスフィルタ機能によるフィルタ処理手順を示すフローチャート図である。

【図4】図2に示すシステムにおけるWebサーバの動作を示すフローチャート図である。

【図5】図2に示すシステムで用いられるフィルターテーブルの登録内容の一例を示す図である。

【図6】図2に示すシステムで用いられるフィルターテーブルの登録内容の他の例を示す図である。

【図7】本発明の無線LANシステムに適用可能なコンピュータシステムの一形態を示すブロック図である。

【図8】従来の無線LANシステムの概略構成を示すブロック図である。

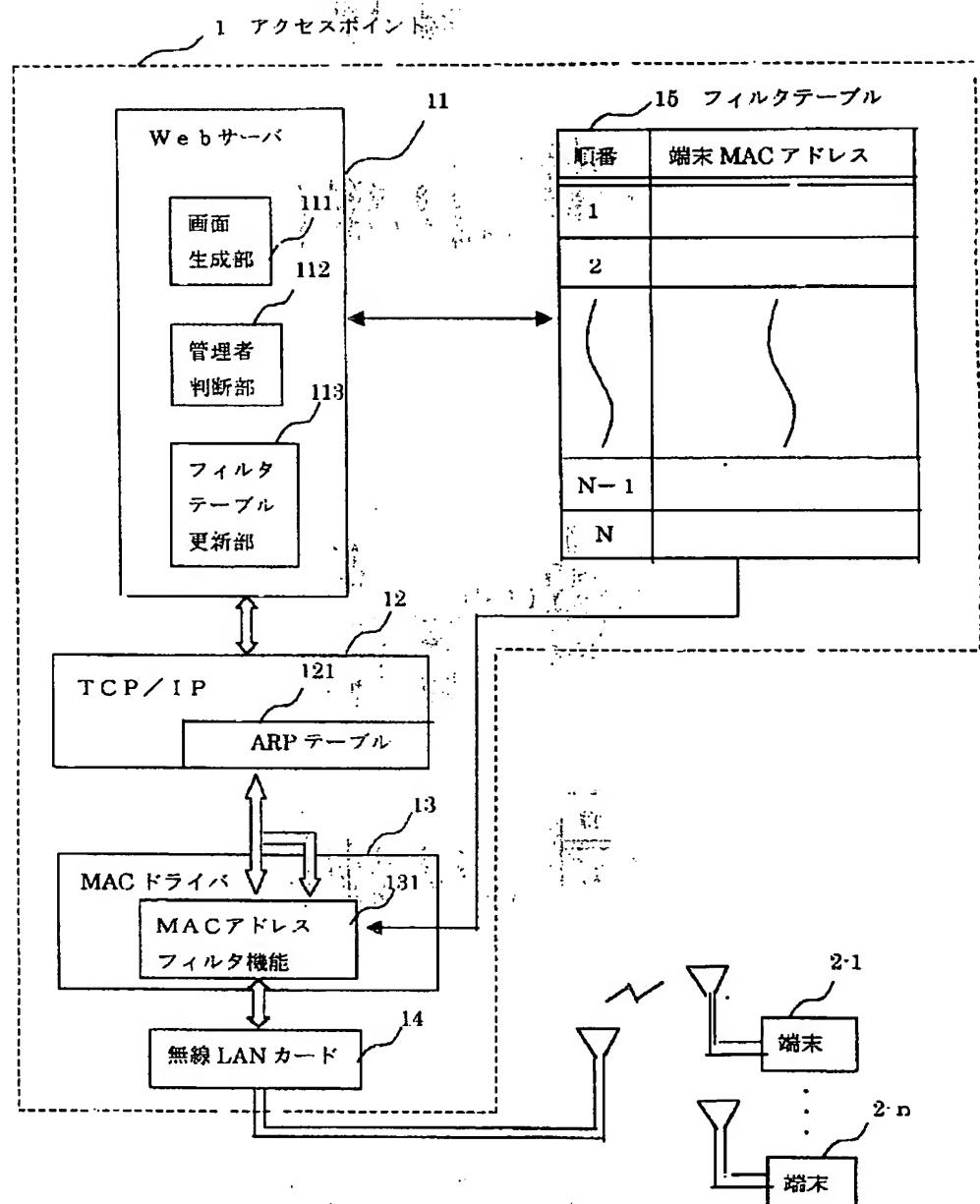
【符号の説明】

- 1 ～ 101 アクセスポイント
- 2-1～2-n、2a、2b 端末
- 11、21 Webサーバ
- 12、22 TCP/IP
- 13、23 MACドライバ
- 14、24 無線LANカード
- 15、25 フィルターテーブル
- 20、Windows共有ファイル
- 30 制御装置

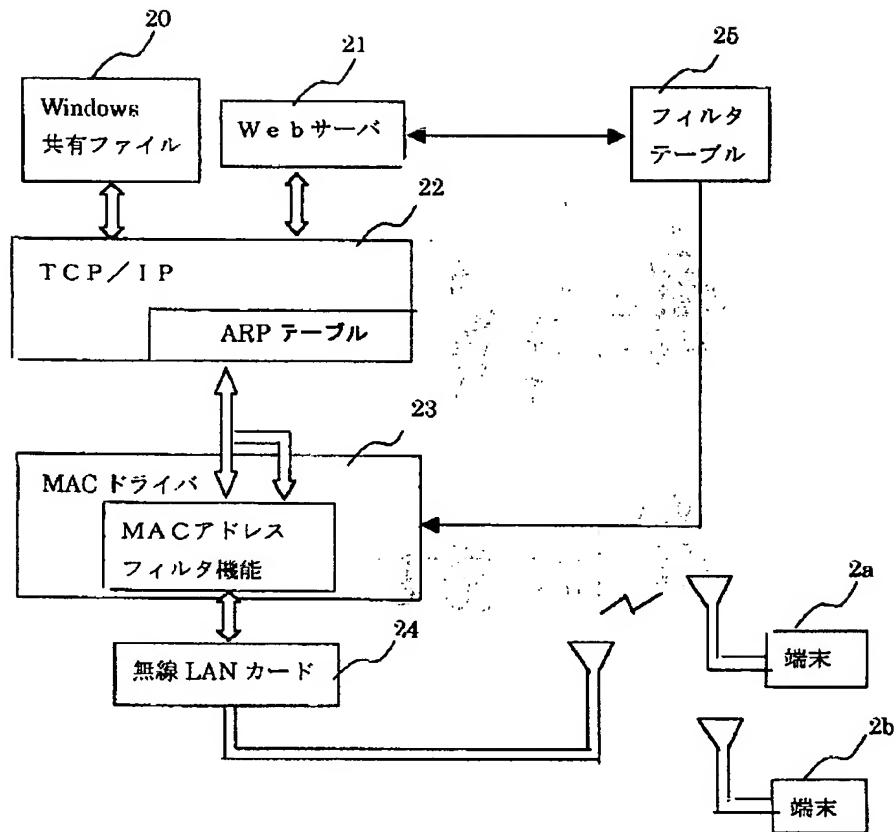
3 1 記憶装置
3 2 入力装置
3 3 表示装置
3 4 通信装置
3 5 出力装置
102-1~102-k STA
104 BBS

105 イーサネット
111 画面生成部
112 管理者判断部
113 フィルタテーブル更新部
121 ARPテーブル
131 MACアドレスフィルタ機能

【図1】



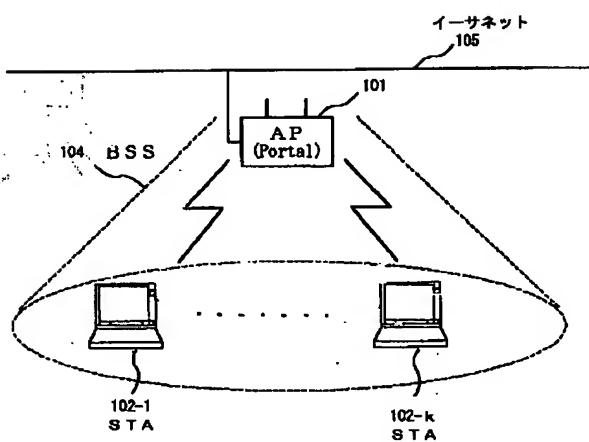
【図2】



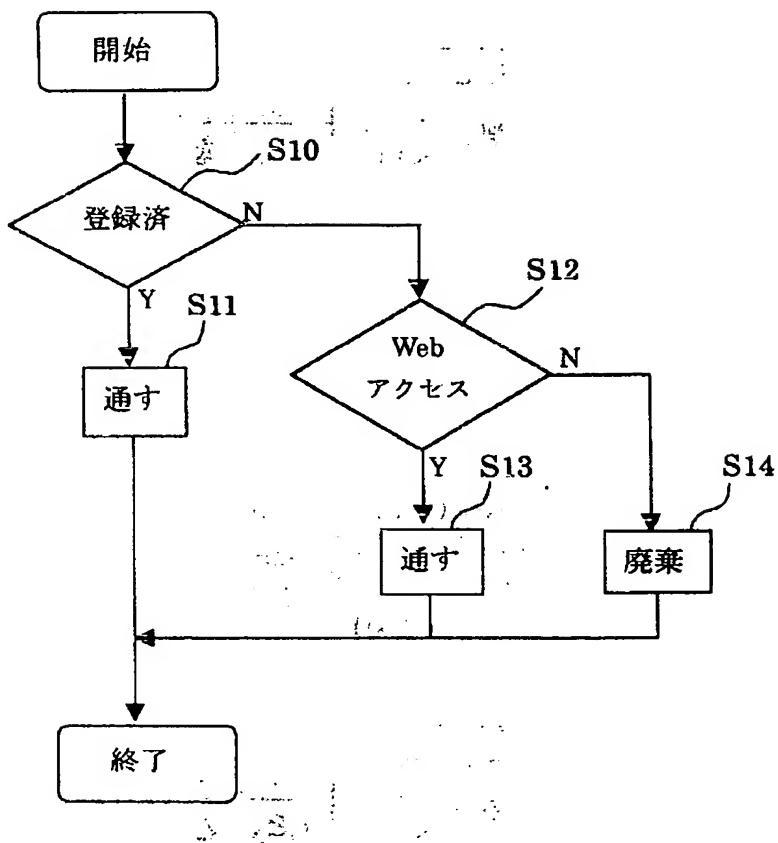
【図5】

順番	MAC アドレス
1	000042-8A9C01
2	000042-8A9C02

【図8】



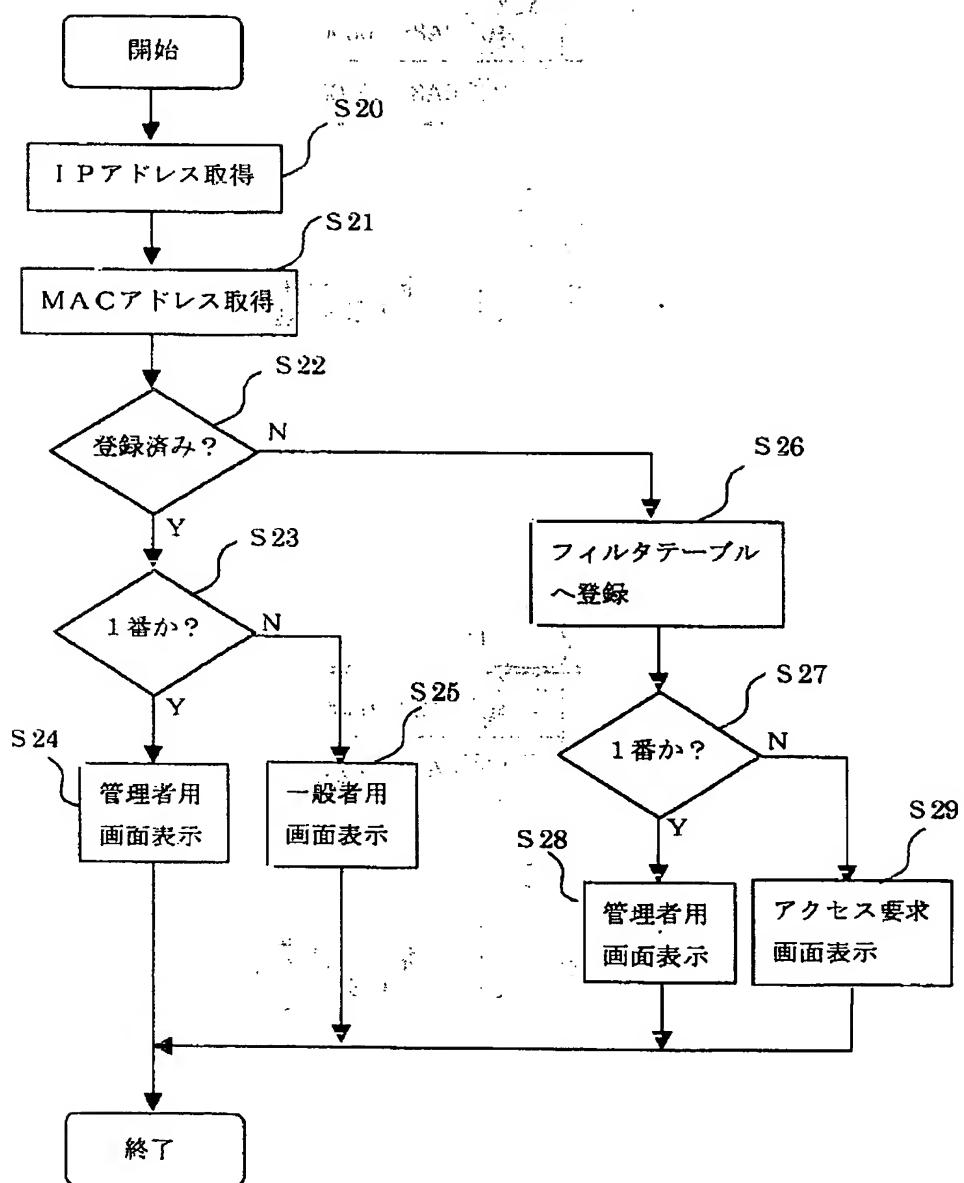
【図3】



【図6】

順番	MACアドレス	設定入力結果
1	000042-8A9C01	
2	000042-8A9C02	アクセス許可

【図4】



【図7】

